IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

VICTOR MALLH
3017 43rd Street, Apt. 3F
Astoria, New York 11103,

Plaintiff, on his own behalf
And similarly-situated others,

v.

EQUIFAX , INC.

Serve Upon:
CORPORATION SERVICE COMPANY
80 State Street
Albany, New York 12207

Defendant.

Case No. 17-5555

CLASS ACTION COMPLAINT AND JURY TRIAL DEMAND

COMES NOW THE PLAINTIFF, on his own behalf, and on behalf of similarly situated others, as defined in this Complaint, and sues the Defendant Equifax, Inc. ("Defendant" or "Equifax") and states:

NATURE OF THE ACTION

1. The Plaintiff and similarly situated others ("the Plaintiffs") bring this matter to address Equifax's unprecedented failure of its duty to protect the most sensitive credit information of eight million New Yorkers. Equifax also failed to provide timely notification to New York State consumers, including the Plaintiffs, that their information had been stolen and the nature and extent of such theft. These acts and omissions violated numerous New York consumer protection laws including NY CLS

Gen Bus § 380-b, NY CLS Gen Bus § 380-k, NY CLS Gen Bus § 380-l, and NY CLS Gen Bus § 380-m.

JURISDICTION AND VENUE

2. Subject-matter jurisdiction is proper in the Court, and is founded upon 28 U.S.C.§1332(A)(1). The Defendant is a corporation, which is domiciled in the State of Georgia. The representative Plaintiff is a citizen of New York, and all members of the proposed class are citizens of New York.

3. Venue in this District is proper pursuant to 28 U.S.C. § 1391. The representative Plaintiff resides in this District and eight million New York consumers have been injured by Defendant's violations. A substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, and Equifax regularly conducts business in this District.

THE PARTIES

4. Plaintiff Victor Mallh is a citizen of the United States and a resident of Queens County, New York. The Plaintiff is a consumer as defined by NY CLS Gen Bus § 380a(b).

5. The named Plaintiff is a victim of the data breach, which was the factual and proximate result of Equifax' negligent and willful conduct, as alleged herein.

6. Defendant Equifax, Inc. is a publicly traded company incorporated under the laws of the State of Georgia. Defendant's principal place of business is in Atlanta Georgia. Defendant regularly conducts business in New York.

PERTINENT FACTS

7. Equifax is a consumer-reporting agency, which collects and maintains data on consumers in the United States and elsewhere. Equifax collects and maintains sensitive personal data of over 820 million consumers worldwide, including at least eight million consumers in New York State.

8. Equifax holds data relating to essentially all aspects of a consumer's marketplace profile. A significant number of people and entities rely on Equifax's credit profiles to evaluate credit worthiness of consumers.

9. Consumers do not provide their private information to Equifax voluntarily yet it is Equifax who controls how it uses and handles private consumer data. Consumers do not have a reasonable way of preventing Equifax from collecting their data, and they cannot control what Equifax chooses to do with or how Equifax handles their private information. Equifax controls when and to whom it discloses private consumer data to. Consumers are forced to rely on Equifax to protect their sensitive data. Therefore, it was and is incumbent upon Equifax to implement and maintain the strongest safeguards to protect this data. Equifax has utterly failed to do so.

10. From at least March 7, 2017 through July 30, 2017, Equifax allowed the over 100 million consumers' sensitive and private information to be exposed and vulnerable to hackers. Equifax relied on certain open-source code (called "Apache Struts") that it knew or should have known was not secure. Although numerous remedies for the vulnerability were available and known to Equifax as of March 7, 2017, Equifax failed to avail itself of these remedies or to employ other compensating security controls sufficient to protect consumers' sensitive data.

11. Hackers were able to access Equifax's computer system from at least May 13, 2017 through July 30, 2017. These hackers potentially stole sensitive data of at least 8 million consumers residing in New York and 143 million consumers overall (the "Data Breach").

12. Equifax first disclosed the Data Breach to the public on September 7, 2017. The Data Breach exposed sensitive and private data of Plaintiff and other New York residents to an unknown number of people. Sensitive data that was exposed includes but is not limited to full names, social security numbers, dates of birth, addresses, and, upon information and belief, credit card numbers, driver's license numbers, and other unknown personally-identifiable information.

13. Equifax could have prevented the Data Breach had it implemented and maintained reasonable safeguards consistent with representations Equifax made to the public, with industry standards, and with the requirements of New York law. Equifax failed to do so.

14. By failing to secure consumer information, Equifax exposed at least eight million New York residents to the risks of identity theft, financial fraud, tax return scams, and other harm. Plaintiff and other affected consumers have spent, and will continue to spend, resources and time attempting to protect against an increased risk of identity theft and/or fraud. The increased risk of identity theft and fraud as a result of the Data Breach also has caused New York consumers emotional harm, substantial fear and anxiety and likely will do so for many years to come.

15. Equifax willfully waited over one month to inform all consumers of the Data Breach. Equifax caused the Plaintiff and other consumers harm by failing to inform

them about the Data Breach in a timely manner. Equifax subjected consumers to actual injury, as these consumers were deprived of their opportunity to meaningfully consider and address issues related to the Data Breach. Equifax also caused consumers, including the Plaintiffs to suffer severe emotional harm while receiving confirmation that Plaintiffs were among those whose personal information was compromised.

16. The Defendant's failure to properly safeguard the information of Plaintiffs and Class Members violates the requirements of NY CLS Gen Bus § 380-b, NY CLS Gen Bus § 380-k, NY CLS Gen Bus § 380-1, and NY CLS Gen Bus § 380-m.

17. Plaintiff Mallh had used Equifax to obtain credit reports in the past, but he did not subscribe to any of Equifax' credit monitoring services. On or about September 8, 2017, Plaintiff Mallh received instructions, which were furnished by Equifax to determine if his personal information was impacted. The Plaintiff received a confirmation that he was one of the individuals who were impacted by the Equifax lapse in procedure. He was thereafter instructed to enroll in credit monitoring service and was requested to provide his credit card information, which Plaintiff declined to do.

18. On September 7th, 2017, Equifax began to offer consumers an allegedly dedicated secure website where consumers could determine if their information was compromised. Equifax also purported to offer consumers "free" credit monitoring through an Equifax product, TrustedID Premier. However, the terms and conditions of that free service require that Plaintiff and other victims submit to arbitration and waive their right to participate in a class action lawsuit. This

egregious conduct on the part of Equifax was designed to trick suffering victims such as the Plaintiff into forfeiting remedies available to them under the law. This was a self-serving act that was not designed to protect consumers.

19. Even after the Data Breach, Equifax continued in its persistent failure to protect the personal information of consumers. Equifax recklessly and negligently made it extremely easy for phishers to imitate their website concerning the Data Breach (equifaxsecurity2017.com, hereinafter "Data Breach Webpage") and obtain sensitive consumer information. Worse, Equifax shockingly *directed consumers* to a link to an imposter website.

20. In creating the Data Breach Webpage, Equifax created a separate website rather than a subdomain of equifax.com. This was an egregious error on the part of Equifax that further increased the security risks to consumers associated with the Data Breach. This was illustrated clearly by Nick Sweeting, a software engineer who created an imitation of equifaxsecurity2017.com in a successful effort to draw attention to the weakness of Equifax's security and to showcase how easy it is for phishers to imitate the Data Breach Webpage and steal consumers' sensitive information. According to Mr. Sweeting:

> Their site is dangerously easy to impersonate…It only took me 20 minutes to build my clone. I can guarantee there are real malicious phishing versions already out there…It's in everyone's interest to get Equifax to change this site to a reputable domain…I knew it would only cost me $10 to set up a site that would get people to notice, so I just did it…. from a trust perspective, there's no way for users to authenticate the real one vs. my server"[1]

---

[1] See https://www.nytimes.com/2017/09/20/business/equifax-fake-website.html?mcubz=3

21.Creating a separate website for the Data Breach Webpage rather than a subdomain of Equifax.com was a key egregious error that put consumers at unnecessary and avoidable risk. Equifax's actions were and are so reckless that they suggest that the Defendant had never anticipated or planned for a data breach. According to cybersecurity experts, creating a subdomain of Equifax.com would have avoided unnecessary security problems because phishers cannot create a page on the equifax.com domain. Therefore, according to these experts, if the Data Breach Webpage were hosted on Equifax.com instead of a separate website, it would be easy for users to determine that the page was legitimate.[2]

22.This suit is maintainable as a class action. The Plaintiff believes that the class that he proposes to represent is so numerous that joinder of all members is impracticable. The Plaintiff asserts that millions of New York consumers have been, and are being, impacted by the Defendant's actions. There are questions of law and fact common to the class, and the claims of the named Plaintiff is typical of the claims of the class. The Plaintiff will fairly and adequately protect the interests of the class.

23.Pursuant to Federal Rule of Civil Procedure 23, the Plaintiff brings this class action and seeks certification of the claims and certain issues in this action on behalf of a Class defined as:

> ***All New York State residents whose personally identifiable information was received by persons - other than those identified in NY Gen. Bus. Law § 380-b - as a result of the Data Breach, which Equifax made known to the public on September 7, 2017.***

---

[2] *id.*

24. Plaintiff reserves his right to amend the Class definition if further investigation and discovery indicates that the Class definition should be narrowed, expanded, or otherwise modified.

25. Defendant uniformly violated the aforesaid NY FCRA Sections as to all members of the Class, including any subclass arising out of the negligent and willful failure to safeguard Plaintiffs' information, such that the questions of law and fact are common to all members of the Class and any subclass.

26. All members of the Class and any subclass were and are similarly affected by the violations of the law and the relief sought herein is for the benefit of Plaintiffs and members of the Class and any subclass.

COUNT ONE: VIOLATION OF N.Y. Gen. Bus. Law § 380, *et seq*.

27. The Plaintiff realleges all of the previous paragraphs and incorporates the same by reference as if fully set forth herein, and further states:

28. For that the New York General Business Law § 380-k sets forth the compliance requirements for business entities such as the Defendant and specifically provides that:

> "Every consumer or reporting agency shall maintain reasonable procedures designed to avoid violations of sections three hundred eighty-b, three hundred eighty-j and three hundred eighty-t of this article and to limit the furnishing of consumer reports to the purposes listed under said section three hundred eighty-b."

29. The reasonable procedures required under § 380-k are designed to ensure that the information concerning consumers is not reported except under the limited circumstances set forth in § 380-b "and no other."

30. That Equifax breached its duty of care in failing to safeguard and secure Plaintiffs' personal information in violation of § 380-m of the General Business Law of New York.

31. The harm to Plaintiff and other consumers began at the time that the unauthorized breaches occurred. The unauthorized disclosure and dissemination of the private credit data was harmful to Plaintiff and other consumers.

32. That Plaintiff also suffered severe mental harm after he was directed to a website by Equifax and after he learned that he was among those individuals whose personal information had been compromised due to Equifax' said willful failures.

33. Equifax also willfully withheld information regarding the Data Breach until September 7, 2017.

34. Because Equifax knew that the Data Breach was likely to occur as a result of its failure to maintain reasonable procedure, and because it acted knowingly and with willful disregard to the rights of New York consumers, the Defendant violated § 380-I. Equifax' willfulness warrants the imposition of punitive damages, costs and fees in addition to Plaintiff's actual damages.

REQUEST FOR RELIEF

WHEREFORE, your Plaintiff, on behalf of himself and similarly situated Plaintiffs, respectfully requests the following relief against the Defendant, Equifax:

A) Issue a temporary restraining order barring Equifax from offering consumers agreements, which contain provisions that compel arbitrations;

B) An order certifying the class of New York consumers as defined hereinabove;

C) An order enjoining Equifax from engaging in the unlawful violations of the law complained of herein;

D) An order requiring Equifax to promptly notify consumers of the nature and extent of any Data Breaches;

E) An order compelling Equifax to use any and all appropriate measures to safeguard, secure and protect the personal information of New York consumers, including the Plaintiffs;

F) An award of actual damages suffered by the Plaintiffs pursuant to §§ 380-l and 380-m;

G) An award of punitive damages pursuant to § 380-l;

H) An award of costs and reasonable attorneys fees; and

I) Any such other and further relief as to this Court may appear just and proper.

JURY TRIAL DEMAND

The Plaintiff respectfully requests a jury trial.

Respectfully Submitted,

THE PLAINTIFFS,

BY:_______/s/____________________

Their Counsel
John Hermina, Esq.
HERMINA LAW GROUP
Laurel Lakes Executive Park
8327 Cherry Lane
Laurel, Maryland 20707
law@herminalaw.com
Tel 301-776-2003
Fax 301-490-7913

Gregory Allen, Esq.
Law Office of Gregory Allen
120 W. Wilson Avenue
Glendale, California 91203
Tel 203-535-4636

Dated: 9/21/17